



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,917	12/07/2005	Thomas Rottschäfer	DE030203US1	9587
65913	7550	09/22/2009	EXAMINER	
NXP, B.V. NXP INTELLECTUAL PROPERTY & LICENSING M/S41-SJ 1109 MCKAY DRIVE SAN JOSE, CA 95131			NGUYEN, TRONG H	
			ART UNIT	PAPER NUMBER
			2436	
			NOTIFICATION DATE	DELIVERY MODE
			09/22/2009	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

# Office Action Summary

**Application No.**

10/559,917

**Applicant(s)**

ROTTSCHAER ET AL.

**Examiner**

TRONG NGUYEN

**Art Unit**

2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 June 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SF/ICE)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. The objection to **claims 1, 8, 11, and 16** has been withdrawn due to Applicants' amendments.

### ***Response to Arguments***

2. Applicants' arguments with respect to **claims 1-17** have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Objections***

3. **Claims 9 and 16** are objected to because of the following informalities:

**Claim 9** recites "a time between the calculating of the at least one round key by the round key generator and the processing external data using the at least one round key is variable". This is unclear because the time between calculating the round key and using the round key to process external data will normally vary due to different key lengths or data sizes. Similar issue also exists in **claim 16**.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 1, 2, 4, 10, 11, and 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui US 5,261,003 (hereinafter "Matsui") in view of Verbauwhede US 2003/0202658 (hereinafter "Verbauwhede").

**Regarding claim 1**, Matsui discloses **a processor that performs an encryption/decryption operation, the processor comprising:** as ["a data communication system with a data scrambling" (Col. 5, lines 44-45, Fig. 1)] **a control device** [selector 24, selector 25, and step counter 26 (Fig. 1)] **that receives at least one initial key, the control device comprising: a memory that temporarily stores the at least one initial key, and at least one external key input that receives the at least one initial key from a source;** as [At the initial state,...the extended key latch 7 supplies the selected extended key corresponding to the given address to the selector 25, and the key is transmitted to the processing block 9 through the selector 25 (Col. 6, line 2 and 12-15)] **a round key generator connected to the control device as** [address calculating circuit 23 and magnification key latch 7 (Fig. 1)] **via least one communication device, as** [Fig. 1] **wherein the round key generator transfers the at least one round key to the memory of the control device;** as [the extended key latch 7 supplies the selected extended key corresponding to the given address to selector 25 (Col. 6, lines 12-14, Fig. 1)] **and at least one encryption/decryption device** as [scramble processing means 33 (Fig. 1, Col. 5, line 65)] **comprising: at least one external data input that receives external data, as** [plaintext 3 (Fig. 1), selector 25 outputs selected extended keys to all of the scramble processing blocks 9-11 in

scramble processing means 33 (Col. 6, lines 14-15, 34-36, Fig. 1)) **an input that receives the at least one round key from the memory of the control device**, as [selector 25 outputs selected extended keys to all of the scramble processing blocks 9-11 in scramble processing means 33 (Col. 6, lines 14-15, 34-36, Fig. 1)] **and at least one external data output that outputs data processed with the at least one round key**, as [scrambled text 4 (Fig. 1)] **wherein the at least one encryption/decryption device and the round key generator communicate solely via the control device**, as [scramble processing means 33 and address calculating circuit 23 and magnification key latch 7 communicate solely using selector 24, selector 25 (Fig. 1)] **and the control device transmits intermediate results to the round key generator to perform calculation of the at least one round key** as [First, the input plaintext 3 is divided into more significant 4 bytes and less significant 4 bytes, and **the less significant 4 bytes are input to the processing block 9 and the address calculating circuit 23 through the selector 24**. The address calculating circuit 23 calculates an address of a extended key to be selected on the basis of the input plaintext data and outputs the calculated address to the extended key latch 7 (Col. 6, lines 4-12)]

Although Matsui discloses the round key generator receives data from the control device to calculate at least one round key [First, the input plaintext 3 is divided into more significant 4 bytes and less significant 4 bytes, and the less significant 4 bytes are input to the processing block 9 and the address calculating circuit 23 through the selector 24. The address calculating circuit 23 calculates an address of a extended key to be selected on the basis of the input plaintext data and outputs the calculated address to

the extended key latch 7 (Col. 6, lines 4-12)), Matsui does not specifically disclose the round key generator receives **the at least one initial key** from the control device to calculate at least one round key. In addition, although Matsui discloses the round key generator performing calculation of the at least one round key, Matsui does not specifically disclose performing **recursive calculation**. Moreover, Matsui does not specifically disclose **a first request line that sends requests from the at least one encryption/decryption device to the control device; and a second request line that sends requests from the round key generator to the control device, wherein the at least one encryption/decryption device and the round key generator both transmit requests on the respective first and second request lines to start the encryption/decryption operator after both requests are met.**

However, Verbaunghede discloses an AES architecture wherein a round key generator (Fig. 2: comprising KEY SCHEDULING MODULE 12 and KEY SCHED. FSM 20) receives at least one initial key (Fig. 2 and par. 0022: KEY) from a control device (Fig. 2: comprising CONTROLLER 14, key entry buffer 27, KEY ENTRY FSM 28, and key register 26) to calculate at least one round key recursively (Fig. 4a, par. 0032). The AES architecture includes a first request line that sends requests (FIG. 5: STATUS) from the at least one encryption/decryption device (Figs. 2 and 5: comprising ENCRYPT. FSM 19 and ENCRYPTION MODULE 10) to the control device (MAIN FSM 14 is located in the CONTROLLER 14); and a second request line that sends requests (Fig. 5: STATUS) from the round key generator (Figs. 2 and 5: comprising KEY SCHED. FSM 20 and KEY SCHEDULING MODULE 12) to the control device, wherein the at

least one encryption/decryption device and the round key generator both transmit requests on the respective first and second request lines (Figs. 2 and 5) to start the encryption/decryption operator after both requests are met (Figs. 2 and 5, pars. 0009, 0034 and abstract: both the at least one encryption/decryption device (comprising ENCRYPT. FSM 19 and ENCRYPTION MODULE 10) and the round key generator (comprising KEY SCHED. FSM 20 and KEY SCHEDULING MODULE 12) transmit requests (status) on the respective first and second request lines to the control device to initiate one round of the AES algorithm wherein the controller controls the operation of the encryption and key scheduling modules such that these two modules operate in parallel and one round is completed per clock cycle).

Verbauwhede and Matsui are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui by having the round key generator receives the at least one initial key from the control device to calculate at least one round key and performs recursive calculation of the at least one round key and by including a first request line that sends requests from the at least one encryption/decryption device to the control device; and a second request line that sends requests from the round key generator to the control device, wherein the at least one encryption/decryption device and the round key generator both transmit requests on the respective first and second request lines to start the encryption/decryption operator after both requests are met for the purpose of supporting

different combination of key-length and data block length (Verbauwhede, par. 0031) and allowing the controller to operate the encryption and key scheduling modules in parallel to perform one round of the AES algorithm in one clock cycle thereby providing low latency and high throughput (Verbauwhede, par. 0023).

**Regarding claim 2**, Matsui in view of Verbauwhede discloses **the processor of claim 1, wherein the at least one communication device further comprises: first release line**; [Verbauwhede, Fig. 5 illustrates one M.I. line] **and first and second data lines** [Matsui, Fig. 1, arrow between selector 24 and address calculating circuit 23 and arrow between step counter 26 and address calculating circuit 23] but does not specifically disclose a second release line.

However, barring any unexpected result from the selection of two release lines, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have two release lines or M.I. lines.

**Regarding claim 3**, Matsui in view of Verbauwhede discloses **the processor of claim 2, wherein the first and second request lines, the first and second release lines, and the second data lines at least partially use a single physical path** [Matsui, Fig. 1, arrow between selector 24 and address calculating circuit 23 or arrow between step counter 26 and address calculating circuit 23 or Verbauwhede, Fig. 5 illustrates one M.I. line]

**Regarding claim 4**, Matsui in view of Verbauwhede discloses **the processor of claim 1, wherein the at least one round key is temporarily stored in the memory of the control device** as [the extended key latch 7 supplies the selected extended key to

the selector 25 and the key is then transmitted to the processing block 9 (Matsui, Col. 6, lines 12-15)].

**Regarding claim 10**, Matsui in view of Verbaudhede discloses **the processor of claim 1, wherein the processor is an Advanced Encryption Standard (AES) coprocessor** [AES architecture for encrypting or decrypting data (Verbaudhede, par. 0007, line 1)]

**Regarding claim 11**, Matsui discloses **a method of performing an encryption/decryption operation using a processor, the method comprising:** as [a data communication method with a data scrambling (Col. 4, lines 5-6)] **"reading at least one initial key into the control device"** as [At the initial state, ...the magnification key latch 7 supplies the selected extended key to the selector 25 (Col. 6, lines 2 and 12-14, Fig. 1)] **"reading external data into the at least one encryption/decryption device"** as [plaintext 3 (Fig. 1), selector 25 outputs selected extended keys to all of the scramble processing blocks 9-11 in scramble processing means 33 (Col. 6, lines 14-15, 34-36 Fig. 1)] **"reading at least one data word needed to calculate at least one round key from at least one storage device of the control device; transferring the at least one data word to the round key generator"** as [the less significant 4 bytes of plaintext data are input to the address calculating circuit 23 through the selector 24 (Col. 6, lines 6-8)] **"calculating at least one round key on the basis of the at least one data word by using the round key generator; transferring the at least one round key to the control device; and storing the at least one round key in the at least one storage device"** as [the address calculating circuit 23 calculates an address of an extended key

to be selected on the basis of the input plaintext data and outputs the calculated address to the extended key latch 7 (Col. 6, lines 8-12, Fig. 1) and the extended key latch 7 supplies the selected extended key corresponding to the given address to selector 25 (Col. 6, lines 12-14, Fig. 1). *Note that an extended key is generated by calculating its address based on the input plaintext data using the address calculating circuit 23. Thus, the calculated key is a function of the input plaintext. As disclosed by Matsui, since the content of the cipher key or the scramble function to be input to the processing block of each step can be varied depending on the content of the plaintext, high random rate can be obtained and thus the possibility of decoding or analysis of the data communication can be reduced (Col. 9, lines 63-68)]* **"transferring the at least one round key from the at least one storage device to the at least one encryption/decryption device"** as [selector 25 outputs selected extended keys to scramble processing blocks 9-11 in scramble processing means 33 (Col. 6, lines 14-15, 34-36, Fig. 1)] **"processing the external data by using the at least one encryption/decryption device, using the at least one round key"** as [scramble processing means 3 scrambles an input data by using an extended key to output a scrambled data (Col. 6, lines 15-17, 36-39, Fig. 1)] **"and the processed data are made available at at least one external data output,"** as [scrambled text 4 (Col. 6, lines 44-48, Fig. 1)] **"repeating the method as often as necessary to encrypt or decrypt a set of external data"** as [the same processing as described above is repeated predetermined times to produce scrambled text 4 (Col. 6, lines 44-48)] **"wherein the control device transmits intermediate results to the round key generator to**

**perform calculation of the at least one round key"** as [First, the input plaintext 3 is **divided** into more significant 4 bytes and less significant 4 bytes, and **the less significant 4 bytes** are **input to** the processing block 9 and **the address calculating circuit 23 through the selector 24**. The address calculating circuit 23 calculates an address of a extended key to be selected on the basis of the input plaintext data and outputs the calculated address to the extended key latch 7 (Col. 6, lines 4-12)].

Matsui does not specifically disclose **sending a first request on a first request line from at least one encryption/decryption device to a control device and a second request on a second request line from a round key generator to the control device to start the encryption/decryption after both requests are met, wherein the at least one initial key is obtained from a source other than the round key generator and round key is calculated recursively.**

However, Verbauwhede discloses an AES architecture wherein a round key generator (Fig. 2: comprising KEY SCHEDULING MODULE 12 and KEY SCHED. FSM 20) receives at least one initial key (Fig. 2 and par. 0022: KEY) from a control device which previously received the at least one initial key from a source other than the round key generator (Fig. 2: comprising CONTROLLER 14, key entry buffer 27, KEY ENTRY FSM 28, and key register 26) to calculate at least one round key recursively (Fig. 4a, par. 0032). The AES architecture includes a first request line to send requests (Fig. 5: STATUS) from the at least one encryption/decryption device (Figs. 2 and 5: comprising ENCRYPT. FSM 19 and ENCRYPTION MODULE 10) to the control device (MAIN FSM 14 is located in the CONTROLLER 14); and a second request line to send requests

(Fig. 5: STATUS) from the round key generator (FIGS. 2 and 5: comprising KEY SCHED. FSM 20 and KEY SCHEDULING MODULE 12) to the control device to start the encryption/decryption operator after both requests are met (Figs. 2 and 5, pars. 0009, 0034 and abstract: both the at least one encryption/decryption device (comprising ENCRYPT. FSM 19 and ENCRYPTION MODULE 10) and the round key generator (comprising KEY SCHED. FSM 20 and KEY SCHEDULING MODULE 12) transmit requests (status) on the respective first and second request lines to the control device to initiate one round of the AES algorithm wherein the controller controls the operation of the encryption and key scheduling modules such that these two modules operate in parallel and one round is completed per clock cycle).

Verbauwhede and Matsui are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui by sending a first request on a first request line from at least one encryption/decryption device to a control device and a second request on a second request line from a round key generator to the control device to start the encryption/decryption after both requests are met, obtaining the at least one initial key is from a source other than the round key generator and calculating round key recursively as described by Verbaughede for the purpose of supporting different combination of key-length and data block length (Verbaughede, par. 0031) and allowing the controller to operate the encryption and key

scheduling modules in parallel to perform one round of the AES algorithm in one clock cycle thereby providing low latency and high throughput (Verbauwhede, par. 0023).

**Regarding claim 17**, this claim contains limitations that are substantially similar to those recited in **claim 10** above and accordingly is rejected for the same reasons.

6. **Claims 5 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Verbauwhede and further in view of Tran US 5,919,251 (hereinafter "Tran").

**Regarding claim 5**, Matsui in view of Verbauwhede discloses **the processor of claim 1** but does not expressly disclose **wherein the at least one round key is accessed using a rotating pointer**.

However, Tran discloses a rotating pointer buffer for storing data in integrated circuits wherein a head pointer and a tail pointer are used to provide access (Col. 1, lines 51, 54-47, Fig. 1).

Tran, Matsui, and Verbauwhede are analogous art because they are in the same field of endeavor of data storage.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify data communication system with a data scrambling of Matsui in view of Verbauwhede by including at least one rotating pointer to provide access to the selected extended key as described by Tran since rotating pointer structure is superior to shifting structure in terms of lowest area consumption and speed (Tran, Col. 2, lines 18-20, Table 1).

**Regarding claim 14**, this claim contains limitations that are substantially similar to those recited in **claim 5** above and accordingly is rejected for the same reasons.

7. **Claims 6-7 and 12-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Verbauwheide and further in view of John L. Hennessy and David A. Patterson, Computer Architecture: A Quantitative Approach, 2nd ed., Morgan Kaufmann, January 1996 (hereinafter "Hennessy and Patterson").

**Regarding claim 6**, Matsui in view of Verbauwheide discloses **the processor of claim 1** but does not expressly disclose **wherein the communication between the control device and the at least one encryption/decryption device and between the control device and the round key generator is accomplished using at least one handshake protocol**.

However, Hennessy and Patterson disclose an asynchronous bus wherein "self-timed, handshaking protocols are used between bus sender and receiver" (Page 499, par. 2, lines 1-2).

Hennessy and Patterson, Matsui, and Verbauwheide are analogous art because they are in the same field of endeavor of computer architecture and data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui in view of Verbauwheide by using handshaking protocols as described by Hennessy and Patterson since it would be much easier to accommodate a variety of devices and to

lengthen the bus without worrying about clock skew or synchronization problems (Hennessy and Patterson, Page 499, par. 3, lines 1-3).

**Regarding claim 7**, Matsui in view of Verbauwhede discloses **the processor of claim 1** but does not expressly disclose **wherein the operation of the of the control device, of the at least one encryption/decryption device, and of the round key generator are asynchronous with respect to one another.**

However, Hennessy and Patterson disclose an asynchronous bus wherein "self-timed, handshaking protocols are used between bus sender and receiver" (Page 499, par. 2, lines 1-2).

Hennessy and Patterson, Matsui, and Verbauwhede are analogous art because they are in the same field of endeavor of computer architecture and data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui in view of Verbauwhede by including an asynchronous bus as described by Hennessy and Patterson since it would be much easier to accommodate a variety of devices and to lengthen the bus without worrying about clock skew or synchronization problems (Hennessy and Patterson, Page 499, par. 3, lines 1-3).

**Regarding claim 12**, this claim contains limitations that are substantially similar to those recited in **claim 6** above and accordingly is rejected for the same reasons.

**Regarding claim 13**, this claim contains limitations that are substantially similar to those recited in **claim 7** above and accordingly is rejected for the same reasons.

8. **Claims 8-9 and 15-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Verbauwhede and further in view of Muratani et al. US 2002/0021802 (hereinafter "Muratani").

**Regarding claim 8**, Matsui in view of Verbauwhede discloses **the processor of claim 1** but does not specifically disclose **wherein the round key generator performs a dummy operation**.

However, Muratani discloses although exemplary configurations of FIG. 1 and FIG. 2 generate a plurality of expanded keys in number required for the data randomizing section, there can comprise the number of stages for round functions capable of generating expanded keys in number that exceeds the number required for the data randomizing section, wherein a part of the generated expanded keys is used by the data randomizing section (par. 0178). Note that non-used expanded keys are dummy operations as Muratani discloses that a configuration in which only part of the expanded keys that are capable of being generated is used for data randomizing is effective in view of safety against attack (par. 0185).

Muratani, Verbauwhede, and Matsui are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui in view of Verbauwhede by having the round key generator performs a dummy

operation as described by Muratani for the purpose of being effective in view of safety against attacks (Muratani, par. 0185).

**Regarding claim 9**, Matsui in view of Verbauwheide discloses **the processor of claim 1** but does not specifically disclose **wherein a time between the calculating of the at least one round key by the round key generator and the processing of the external data using the at least one round key is variable**.

However, Muratani discloses that the order in which the expanded keys are generated may be changed, for example, an earlier generated expanded key may be temporarily stored in a memory to be used later than a later generated expanded key (Fig. 15, Col. 9, Par. 0197, lines 4-5, Par. 0199, lines 1-3).

Muratani, Verbauwheide, and Matsui are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui in view of Verbauwheide by including **wherein a time between the calculating of the at least one round key by the round key generator and the processing of the external data using the at least one round key is variable** as described by Muratani for the purpose of being effective in view of safety against attack (Muratani, par. 0197).

**Regarding claim 15**, this claim contains limitations that are substantially similar to those recited in **claim 8** above and accordingly is rejected for the same reasons.

**Regarding claim 16**, this claim contains limitations that are substantially similar to those recited in **claim 9** above and accordingly is rejected for the same reasons.

### ***Conclusion***

Applicants' amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/  
Supervisory Patent Examiner, Art Unit 2436

/T N/  
Examiner, Art Unit 2436